#31 Appeal
1-29-04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	09/281,042	Confirmation No. 6678
Applicant	:	Seiki Aguro	
Filed	:	03/30/1999	
TC/A.U	:	2123	
Examiner	:	Jones, Hugh M	
Docket No.	:	TIJ-26495	
Customer No.	:	23494	

APPEAL BRIEF

MAILING CERTIFICATE UNDER 37 C.F.R. §1.8(A)
I hereby certify that the above correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to: Mail Station AF, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.

William B. Kempler 11/16/04
William B. Kempler Date:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The following Appeal Brief is respectfully submitted in support of an appeal of the final rejection of Claims in connection with the above-identified application. The final Rejection was mailed 11/19/2003.

REAL PARTY IN INTEREST

01/29/2004 THALL1 00000001 200660 09281042
04 FC:1402 320.00 DA

The invention has been assigned to Texas Instruments Incorporated.

RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to Applicant's representative which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

STATUS OF THE CLAIMS

Claims 4-21 stand rejected. Claims 1-3 were filed with the application and amended on filing by a preliminary amendment. Claims 1-3 were cancelled by the amendment dated 03/26/2001 and were replaced by new Claims 4-21. Claims 4-21 were rejected in the final rejection of 06/19/2001. Claims 4 and 8 were amended in the amendment dated 10/01/2001. In the Advisory Action of 10/23/2001 the Examiner complained that a "marked up copy" was not provided although one was submitted with the 10/01/2001 amendment. A copy of the marked up version of the Claims was sent along with the Notice of Appeal with a request that the amended Claims be entered because they only corrected typographical errors and were therefore in a better form for appeal. The original Advisory Action indicated that the Examiner accepted none of Applicant's arguments but indicated, that on filing an Appeal, Claims 4-21 are allowed. A new Advisory Action mailed 5/31/2002 indicates that Claims 4-21 stand rejected.

Prosecution on the merits was reopened by an Official Action dated March 14, 2003 which was based on the Appeal Brief and Petition to the Commissioner of Patents Under 37 C.F.R. 1.181 mailed July 1, 2002 and the Decision on Petition dated 08/15/2002. Claims 4-21 were rejected and Claims 4, 8, 9, 11, 13 and 14 amended. Claims 4-21 stand rejected.

STATUS OF THE AMENDMENTS

The application was filed with Claims 1-3, which were amended on filing by a preliminary amendment. These Claims were cancelled by the amendment dated

03/26/2001 and replaced by Claims 4-21. Claims 4 and 8 were amended in an amendment dated 10/01/2001, which has now been entered by the Examiner in the Advisory Action mailed 6/03/2002. Claims 4-9, 11, 13 and 14 were amended in a response mailed 02/19/2002. No response to the Final Rejection of 11/19/2003 has been filed. A Petition to the Commissioner of Patents Under 37 C.F.R. 1.181 has been filed concurrently herewith concerning the Examiner's objections to Claims 5-7, 10-13 and 15-17.

SUMMARY OF THE INVENTION

The present invention is related to preventing access to the program stored within a one-chip computer system. It is common to provide security for a computer system via a password and a limitation on the number of tries to input the correct password. This works in a fixed system environment. In a one-chip computer environment, this method will fail because there is a large number of systems available on which attempts for unauthorized access may be tried.

The present invention provides a simple yet effective solution to the problem by having the processor utilize a stored program to receive and process a plurality of commands applied to a plurality of input ports to the processor to generate the password (page 14, lines 3-25, page 15, lines 8-23 and page 16, lines 15-23). This permits the commands to be applied in a described sequence, which makes cracking the password far more difficult without the necessity of complex circuitry dedicated to security.

Regarding the elements of claim 4, the processor interconnected with memory and peripheral circuits is described in the specification at page 4, lines 21-24 and page 6, lines 19-22. The scan-path interface is supported at page 4, lines 25-27 and page 8, lines 15-21. The switching circuit is described at page 5, lines 1-6 and page 8, lines 1-5. The plurality of input ports for the processor is supported at page 15, lines 8-12. The program stored in memory is described at page 16, lines 15-23 and the switching circuit being responsive to the comparison can be found at page 10, lines 14-22.

Regarding Claim 8, see page 15, lines 8-12 for support for the plurality of input ports for the processor. See page 16, lines 15-23 for a description of the remainder of the elements of the claim.

Regarding Claim 14, the means for applying is described at page 15, lines 8-12. The program stored in memory and the means for comparing are found at page 16, lines 15-23.

ISSUES

The issues on appeal are whether Claims 8, 10 and 14-15 omit both an essential step and/or an essential structural cooperative element, whether Claims 8, 10 and 14-15 are anticipated by Palmer, Jr., et al, whether Claims 8, 10 and 14-15 are anticipated by Angelo, whether Claims 4, 5, 9 and 15 are unpatentable over Palmer, Jr. et al. in view of Raghavachari, whether Claims 6, 7, 11-13, 16, 17, 19-21 are unpatentable over Palmer, Jr., et al. in view of Raghavachari and further in view of Jacobsen, et al., whether Claim 18 is unpatentable over Palmer, Jr., et al. in view of Jacobsen, et al. and whether Claims 4-7, 9, 11-13 and 16-21 are unpatentable over Angelo in view of Branco, et al.

GROUPING OF THE CLAIMS

Each of the following groups of Claims, as contained in the attached Appendix, are independently patentable, and the rejected Claims of these groups stand or fall together for the reasons more clearly set forth hereinbelow:

Group I	Claims 8, 9, 11, 12
Group II	Claims 10, 13
Group III	Claims 14, 16, 18
Group IV	Claims 15, 17, 19-21
Group V	Claims 4, 6
Group VI	Claims 5, 7

Group I contains Claims 8, 9, 11, 12 which stand or fall together.

Group II contains Claims 10 and 13 which stand or fall together. Claim 10 recites that the processor in Claim 8 receives the plurality of commands which are applied to the plurality of ports in a specific time sequence. This additional feature is not shown or suggested by

the references of record and provides a significant improvement over the prior art by making the code more secure.

Group III contains Claims 14, 16 and 18 which stand or fall together. Claim 14 recites means for applying a plurality of commands to a plurality of ports for a processor of the system. This feature is not found in any of the Claims discussed above and makes Claim 14 separately patentable as none of the references of record show or suggest this feature.

Group IV contains Claims 15, 17, 19-21 which stand or fall together. Claim 15 recites the feature that the processor receives the plurality of commands which are applied to the plurality of ports in a specific time sequence. This feature is not shown or suggested in the art of record making Claim 15 separately patentable. This feature, when combined with the features of Claim 14 from which it depends, recites a patentable combination separate from the Claims discussed above.

Group V contains Claims 4 and 6 which stand or fall together. Claim 4 specifically recites a processor interconnected with memory and peripheral circuits on the integrated circuit, a scan-path interface circuit for reading out contents of a predetermined memory or register of the system and a switching circuit coupled to the processor and the scan-path interface circuit. The Claims discussed above do not specifically recite the processor interconnected with a memory and peripheral circuits on the integrated circuit or that the scan-path interface circuit is for reading out the contents of a memory or register of the system and that the switching circuit is coupled to the processor and the scan-path interface circuit. The recitation of these features makes Claim 4 separately patentable.

Group VI contains Claims 5 and 7 which stand or fall together. Claim 5 recites a program that operates the processor to receive the plurality of commands applied to the plurality of ports in a specific time sequence. This feature when combined with the features of Claim 4 from which Claim 5 depends, has features not discussed above which render Claim 5 to be separately patentable.

ARGUMENTS

35 USC § 112, second paragraph rejection

The Examiner rejects Claims 8, 10, and 14-15 under 35 U.S.C. § 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. The Examiner rejects the same Claimsunder 35 U.S.C. § 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between necessary structural connections.

In paragraph 46 of the Official Action mailed 11/19/2003, the Examiner states that Claim 8 is a "system" claim and includes apparatus and steps. The Examiner states that the amendment does not cure the deficiency. The Examiner has not commented on independent Claim 14.

Independent Claims 8 and 14 are written in the "means plus function" format. Thus, the recitation of the function does not convert this element to a method step and is specifically provided for in 35 U.S.C. §112, paragraph 6.

35 U.S.C. §102 rejections

The Examiner rejects Claims 8, 10 and 14-15 under 35 U.S.C. §102(b) as being clearly anticipated by Palmer, Jr., et al. The Examiner states with regard to Claim 8, the reference discloses an integrated circuit computer system shown in Figure 2, item 6i having a processor interconnected with memory shown in Figure 1, item 6d and peripheral circuits on the integrated circuit, Figure 1, items 6f, 6c and 6a coupled to a security system. With regard to Claim 14, Examiner states that the reference shows a security system for integrated circuit computer system for applying a plurality of commands to a plurality of ports for the processor and refers to Figure 1, items 6a, the block labeled PROCESS CONTROL PROGRAM, item 4, item 6f, a program stored in a memory coupled to the processor to process to a plurality of commands to produce a password shown in Figure 2, items 6i, 6c and comparing the produced password with a predetermined password shown in Figure 1, item 6 and Figure 2, item 6i.

First of all, it must be noted that, referring to the brief description of the figures in Palmer, Jr., et al., Figure 1 is not a block diagram for the system, but is a flow diagram for the data in the system. Claims 8 and 14 are device claims, or in the Examiner's opinion "system" claims, and for a '102 rejection, the elements of these claims will have to be found in this single reference. The Examiner's first error is to assume that items 6b, 6d and 6e are inputs to the processor which he is obviously reading on the process control program (unlabeled in Figure 1). Figure 2 is a block diagram of the system. It is clearly shown in Figure 2 that items such as the operating system program, the look-up table and constants' table are stored in the 1024 byte ROM and the software clock, parameter storage are stored in the 64 byte RAM. Thus, they are not inputs to the signal chip microcomputer which is clearly shown as item 6i and contains the ROM and RAM memories. Referring to Figure 2, element 6i is referred to as "signal chip microcomputer", which indicates that item 6i is a single integrated circuit. The peripheral circuit which the Examiner states are integrated on the chip are the appliance access control unit 6f, which is clearly shown as a separate device and the optical card reader 6c. Those skilled in the art know that an optical card reader cannot be integrated onto an integrated circuit chip. Furthermore, the clock and data outputs of the optical card reader 6c are applied to the test inputs T0 and T1, respectively of the single chip microcomputer, which indicates that they are outside of the integrated circuit chip and thus do not meet the requirements of Claim 8.

In paragraph 11 of the final rejection, the Examiner does refer to Figures 1-3 of Palmer, Jr., et al. Figure 3 is a schematic diagram of the access control module, as clearly shown from the brief description of the figures, a typographical error in column 2, line 55 referring to Figure 2, notwithstanding. In Figure 3 there is a single data input bus shown as pins 1-9 of connector J2 for conveying signals data 0 through data 7 and strobe bar to the microcomputer U2. The optical card, which is an external device, is coupled to the microcomputer U2 via test terminals T0 and T1.

The Examiner refers to item 6c in this rejection and in a further rejection based on this reference in paragraph 20 of the official action, the Examiner refers to items 4 and 6c. These items are the card reader 4 and the card reader portion of the access control module 6, respectively. Referring now to Figure 2 of the cited reference, the optical card reader 6c is coupled to the single chip microcomputer 6i via a clock line and a data line

which forms a first port. The password entered via the optical card reader is compared with a password stored in the ROM of the single chip microcomputer, which is internal to the microcomputer, as clearly shown in Figure 2, and discussed above. Accordingly, applying this reference to the present invention, the "command" would be applied to the test port T0, T1; would be read by the single chip microcomputer and compared to a password stored in its memory. There is no showing of the password being generated by a plurality of commands applied to a plurality of ports for the processor. Just to make sure that the concept of "port" is clear, applicants previously submitted a portion of the text "Imbedded Microprocessor Systems - Real World Design" by Stuart R. Ball and include a copy herewith. Furthermore, applicants had previously submitted a copy of a portion of the text "Programming Embedded Systems I" by Michael J. Paunt which clearly shows on page 1-12 that standard 8051s (microprocessors) have four 8-bit ports, all the ports being bidirectional. A copy is included herewith. Therefore, it should be clear that a "port" is a group of I/O pins on a microcomputer chip which operate together for a particular function.

Thus, the fact that the store computer system inputs a "seed" into the access control module of the cited reference is irrelevant here because the seed and the clock output are used to find the password stored in the computer which is compared to the input password. Therefore, even if one were to ignore the arguments above and characterize the seed as a second command, it would not anticipate the present invention or render it obvious because it is not used to generate the password, which is read by the optical card reader. Although the Examiner has not specifically discussed the possibility, even if one were to reverse the situation in which the seed were read in through the optical card reader and the password came in through the main computer interface port, the situation would not change, because the information coming through the main computer interface port is a "seed" which is combined with an output of the clock to produce a pointer to the password. The hardware system clock and software clock are both shown in Figure 2 as being internal to the single chip microcomputer 6i and thus do not come from a second port.

In view of the fact that Claim 8 recites applying a plurality of commands to a plurality of ports and having the program operating the processor or being operable to

control the processor to process the plurality of commands to produce a password, Claim 8 is clearly distinguished from this reference. Claim 14 recites "means for applying a plurality of commands to a plurality of ports for a processor of said system "which is not shown or suggested by Palmer, Jr., et al. Claim 10 recites that the processor in Claim 8 receives the plurality of commands which are applied to a plurality of ports in a specific time sequence. This additional feature is not shown or suggested by Palmer, Jr., et al. and provides a significant improvement by making the code more secure without the need for additional circuitry. Similarly Claim15, which is dependant on Claim 14, recites this same feature and is therefore separately patentably distinct from Palmer, Jr., et al.

The Examiner rejects Claims 8, 10 and 14-15 under 35 U.S.C. 102(e) as being clearly anticipated by Angelo. The Examiner states that Angelo discloses a method for enabling power to all portions of a computer system based upon the results of a two-piece user verification process that is completed as part of a secure power-up procedure. The Examiner specifically highlights portions of the text which recites that at some point during the secure power-up procedure, the computer user provides an external token or smart card that is coupled to the computer using specialized hardware and that the computer user is required to enter a plain text user password or, a password generated by the aid of biometrics.

This rejection is respectfully traversed. First of all, the Angelo reference is not to an integrated circuit computer system, as required by Claims 8 and 14. The system described in Angelo at col. 3, lines 48-58 includes bay door/case locks and mass data storage devices. The system provides security by withholding power to the peripheral devices and to the bay door/case locks forcing the possessor of a stolen computer to physically damage the computer casing. Accordingly, this reference is not applicable to the present invention, where such devices can not exist. Furthermore, a '102 rejection requires all elements of the claim to be present, which is clearly not true here. Moreover, the two-piece nature of the authorization process, does not require utilization of applying commands to two input ports on a processor. In fact, referring to Figure 1, we see that the floppy/keyboard controller 136 has coupled thereto a keyboard 159 via keyboard connector 158 and a probe 186, into which the token 188 is plugged, is coupled to the floppy/keyboard controller 136 via an RS-232 connector 146 and a com port adapter 184.

Accordingly, both of the inputs into the system that are required, that is, the token and the typed in password, pass through the floppy/keyboard controller 136 and via a single bus into the port comprising lines 106 and 108. Therefore, this reference fails to show or suggest the application of a plurality of commands to a plurality of ports for generating a password, as required in Claim 8. Nor does it show or suggest the "means for applying a plurality of commands to a plurality of ports of said system "required by Claim 14. Claim 10 recites that the processor in Claim 8 receives the plurality of commands which are applied to a plurality of ports in a specific time sequence. This additional feature is not shown or suggested by Palmer, Jr., et al. and provides a significant improvement by making the code more secure without the need for additional circuitry. Similarly Claim15, which is dependant on Claim 14, recites this same feature and is therefore separately patentably distinct from Palmer, Jr., et al.

35 U.S.C. 103 rejections

The Examiner rejects Claims 4, 5, 9, and 15 under 35 U.S.C. 103(a) as being unpatentable over Palmer, Jr. et al in view of Raghavachari. The Examiner states that Palmer, Jr. et al does not expressly disclose a scan-path interface circuit for reading out a predetermined memory or register in the system and that this is disclosed in Raghavachari. The Examiner concludes that it would have been obvious to one of ordinary skill in art at the time the invention was made to combine the two references.

This rejection is respectfully traversed. First of all, the discussion above concerning Palmer, Jr. et al applies here and Claim 4 clearly requires a plurality of commands applied to a plurality of input ports on a processor to process the commands to produce a password, which is not shown by Palmer, Jr. et al.

Furthermore, with regards to Raghavachari, Figure 1 clearly shows that all input to the system comes through the port comprising lines TCK, TMS and TDI. These lines come through the boundary scan-port and control 15. No other input lines are shown. Therefore, these lines comprise the only input port to the device. Accordingly, this reference can not show or suggest the application of a plurality of commands to a plurality of input ports and processed to generate a password, as required by Claim 4. In

fact, since both references show the utilization of a single port, the combination teaches away from the present invention.

The Examiner states that with regard to Claim 9, Palmer, Jr. et al does not expressly disclose a switching circuit coupled to the scan-path interface. The Examiner states that Raghavachari discloses that many integrated circuits are accessed via scan-ports and specifically discloses a switching circuit coupled to the scan-path interface. The Examiner concludes that it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Palmer, Jr. et al with Raghavachari.

Assuming, arguendo, that Palmer, Jr. et al and Raghavachari were to be combined, this still would not teach the utilization of applying commands to a plurality of ports to be processed into a password because Raghavachari only shows a single input port and Palmer, Jr. et al., which does show two input ports, shows them each being used for separate purposes. Accordingly, even if these two devices could be combined, it would not yield the present invention or suggest the present invention.

The Examiner states with regard to Claim 5, the Palmer, Jr. et al reference inherently discloses a specified time sequence.

The "sequence" of Palmer, Jr. et al would that the input through main computer interface 6a would have to occur at a time previous to the input to card reader 4, 6c. However, the reference fails to show or suggest the application of a plurality of commands applied to a plurality of input ports in a specific time sequence to be processed into a password, as would be required by the combination of Claims 4 and 5.

Claim 15 recites that the processor receives a plurality of commands which are applied to the plurality of ports in a specific time sequence. As discussed above, the combination of the two references fails to show or suggest the use of a plurality of ports and therefore Claim 15 is patentably distinct from this combination of references.

The Examiner rejects Claims 6, 7, 11, 12, 13, 16, 17, 19, 20 and 21 under 35 U.S.C. 103(a) as being unpatentable over Palmer, Jr. et al in view of Raghavachari and further in view of Jacobson, et al. These claims are dependent upon Claims 4, 8 or 14, the patentability of which has been discussed above. These claims are patentable for the same reasons.

The Examiner rejects Claim 18 under 35 U.S.C. 103(a) as being unpatentable over Palmer, Jr. et al in view of Jacobson, et al. Claim 18 is dependent upon Claim 14. The patentability of Claim 14 over the Palmer, Jr. et al reference having been discussed above, Claim 18 is patentable for the same reasons.

The Examiner rejects Claims 4-7, 9, 11-13 and 16-21 under U.S.C. 103(a) as being unpatentable over Angelo in view of Bianco, et al. The Examiner states that Angelo discloses a method for enabling power to all or portions of a computer system based on the results of a 2-piece user verification process that is completed as part of a secure power-up procedure. The Examiner states that Angelo does not expressly disclose a scan-pass interface circuit for comparison for a predetermined memory or register and a switching circuit is responsive to the comparison. The Examiner states that Bianco, et al. discloses a set/scan test capability which is provided for a circuit that includes sensitive subcircuits that can be latched out to prevent reverse engineering of the sensitive elements. The Examiner states that various implementations are possible, such as fusable-link PROMs for irreversibly inhibiting set/scan access to the sensitive subcircuits, the use of encryption codes to enable repeated set/scan access to the sensitive subcircuits and an erasable/reprogrammable mechanism for inhibiting set/scan access. The Examiner concludes that it would have been obvious to one of ordinary skill in the art, at the time of the invention, to have modified the Angelo reference with the Bianco, et al. reference.

This rejection is respectfully traversed. The Angelo reference has been discussed above in connection with the rejection of Claims 8, 10 and 14-15. As stated above, Angelo specifically shows all of the inputs needed to generate the password coming through a single input port to the processor. With respect to Bianco, et al, the Examiner specifically points to Figure 6. Figure 6 does show a CPU connected to a system to protect sensitive information from a data scan. However, reading the remainder of the reference, it is clear the protection is provided by an encryption program stored in EEPROM 58. Once the device has been tested by the manufacturer, the system is programmed to bypass the data stored in the sensitive area unless a code equal to that stored in the EEPROM is applied. There is nothing in this reference that shows or even suggests the application of a plurality of commands to a plurality of ports for the

processor 50 to be processed into a password. The password goes through the S/S control 14. Furthermore, the system of Bianco, et al requires considerable additional circuitry to that of the present invention. In fact, the elegance of the present invention is that no additional circuitry is required, it utilizes attributes of the microprocessor that are already present to provide the additional security. Therefore, this reference singly, or in combination Angelo does not show or suggest the present invention. Accordingly, the present claims already clearly distinguished from these references either singly or in combination.

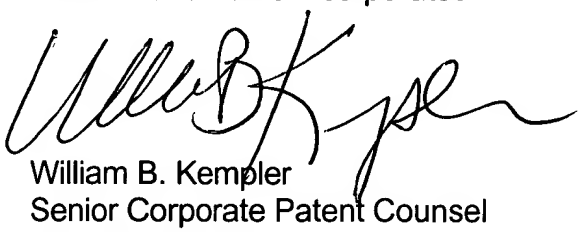
Claim 4 specifically recites that the security mechanism receives a plurality of commands applied to a plurality of input ports which are processed to produce a password, which is not shown or suggested by the combination of references. Claim 11 is dependent from Claim 8 which also recites that the processor receives a plurality of commands at a plurality of input ports which are processed to produce a password. Claim 12 is also indirectly dependant from Claim 8 and is therefore patentable for the same reasons. Claim 13 is dependant from Claim 10 which adds that the receipt of the plurality of commands applied to the plurality of ports is in a specific time sequence. Claim 13 is therefore patentably distinct from the combination of references. Claim 16 is dependant form Claim 14 which recites means for applying a plurality of commands to a plurality of ports and a program stored in memory coupled to the processor for processing the commands to produce a password. It is therefore patentably distinct from the combination of references. Claim 17 is dependent form Claim 15 which recites that the plurality of commands are applied to the plurality of ports in a specific time sequence. Claim 17 is therefore patentably distinct from the combination of references. Claim 18 is dependent from Claim 14 which recites means for applying a plurality of commands to a plurality of ports for a processor and a program stored in memory coupled to the processor which processes the commands to produce a password and is therefore patentably distinct. Claims 19-21 are dependant from Claims 15-17, respectively and are therefore patentable for the same reasons.

CONCLUSION

For the above reasons, Applicants respectfully submit that the Examiner's Final Rejection of Claims 4-21 under 35 U.S.C. § 102, 35 U.S.C. § 103 and 35 U.S.C. § 112, second paragraph are not properly founded in law. Applicants respectfully request that the Board of Patent Appeals and Interferences so find and reverse the Examiner's rejections of the Claims.

Respectfully submitted,

Texas Instruments Incorporated



William B. Kempler
Senior Corporate Patent Counsel
Reg. No. 28,228
(972) 917-5452

APPENDIX

4. An integrated circuit computer system comprising:

a processor interconnected with memory and peripheral circuits on said integrated circuit;

a scan-path interface circuit for reading out contents of a predetermined memory or register in said system;

a switching circuit coupled to said processor and to said scan-path interface circuit for switching said scan-path interface circuit between a first mode in which it is enabled and a second mode in which it is disabled; and

a security mechanism comprising:

a plurality of input ports for said processor;

a program stored in said memory to operate said processor to receive a plurality of commands applied to said plurality of input ports and to process said commands to produce a password which is compared with a predetermined password;

and wherein said switching circuit is responsive to said comparison.

5. The computer system of claim 4 wherein said program operates said processor to receive said plurality of commands which are applied to said plurality of ports in a specific time sequence.

6. The computer system of claim 4 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

7. The computer system of claim 5 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

8. In an integrated circuit computer system having a processor interconnected with memory and peripheral circuits on said integrated circuit, a security system comprising:

a plurality of input ports for said processor;

a program stored in said memory and operable to control said processor to receive a plurality of commands applied to said plurality of input ports and operable to control said processor to process said commands to produce a password which is compared with a predetermined password.

9. The security system of claim 8 further comprising a switching circuit coupled to a scan-path interface circuit and being responsive to said comparison for switching said scan-path interface circuit between a first mode in which it is enabled and a second mode in which it is disabled.

10. The security system of claim 8 wherein said program operates said processor to receive said plurality of commands which are applied to said plurality of ports in a specific time sequence.

11. The security system of claim 8 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling a switching circuit.

12. The security system of claim 9 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling said switching circuit.

13. The security system of claim 10 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers for controlling a switching circuit.

14. A security system for an integrated circuit computer system comprising:

means for applying a plurality of commands to a plurality of ports for a processor of said system;

a program stored in a memory coupled to said processor and operable to control said processor to process said plurality of commands to produce a password;

means for comparing said produced password with a predetermined password.

15. The security system of claim 14 wherein said program is operable to control said processor to receive said plurality of commands which are applied to said plurality of ports in a specific time sequence.

16. The security system of claim 14 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers and generating a comparison signal.

17. The security system of claim 15 further comprising a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers and generating a comparison signal.

18. The security system of claim 14 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and disabled modes.

19. The security system of claim 15 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and a disable modes.

20. The security system of claim 16 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and a disable modes.

21. The security system of claim 17 further comprising a scan-path interface circuit for reading out contents of a predetermined memory or register in said system and a switching circuit responsive to said comparison to switch operation of said scan-path interface circuit between enabled and a disable modes.